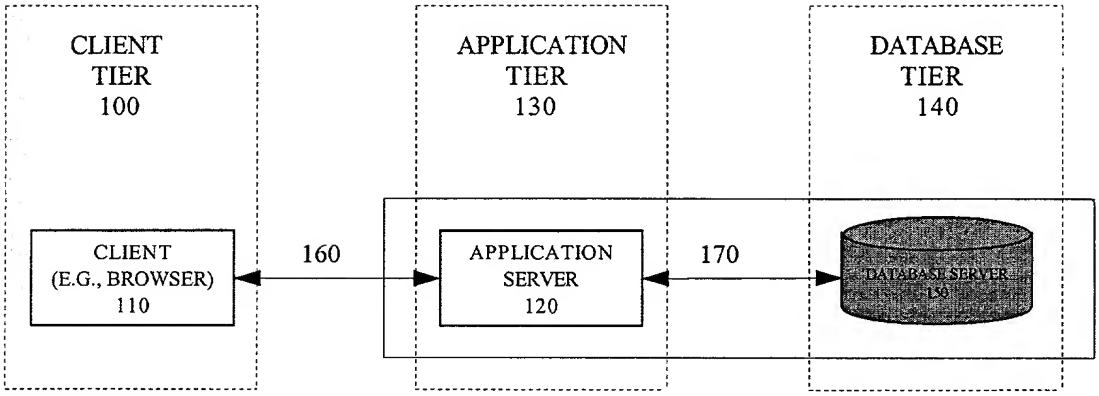
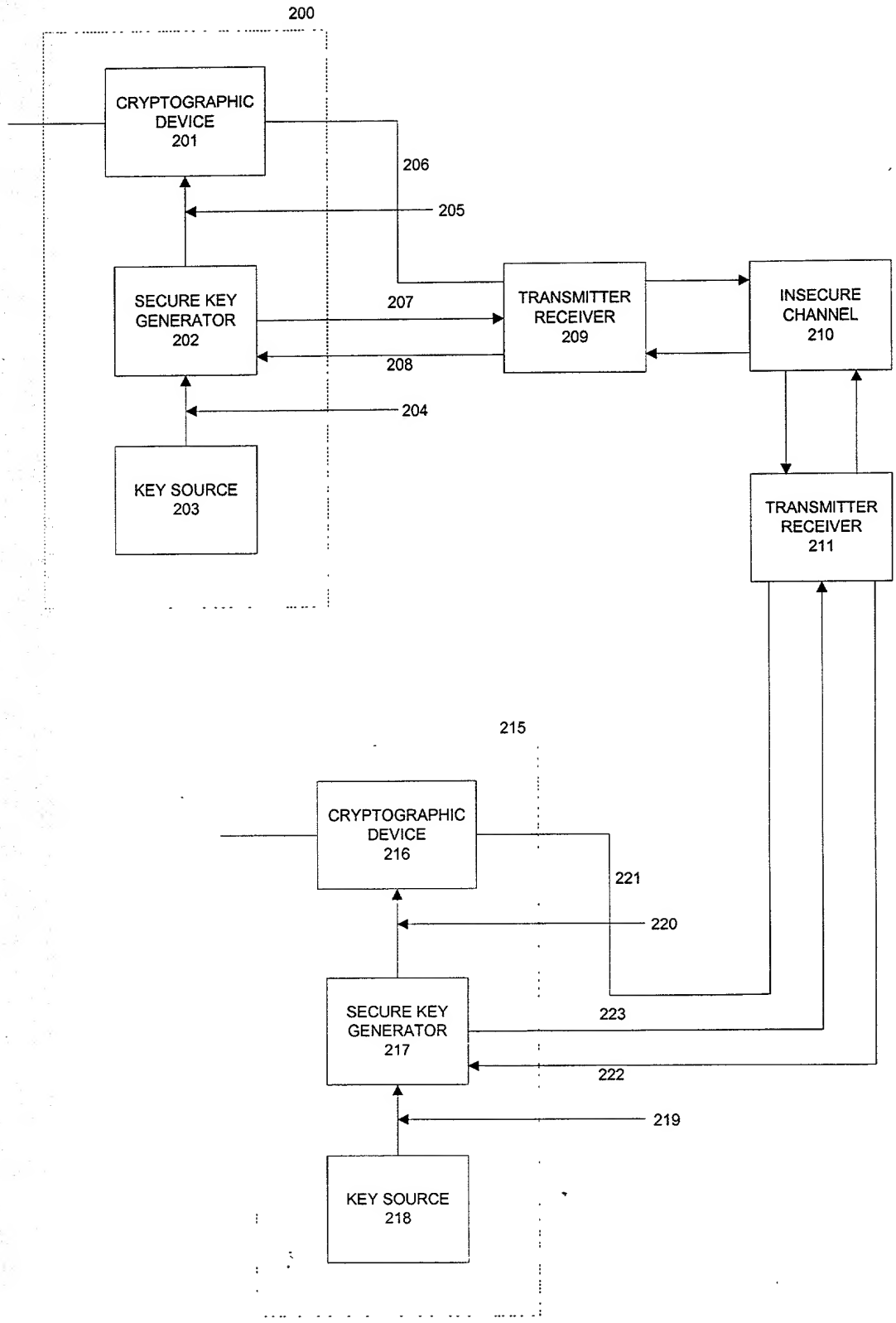

CLIENT
TIER
100
APPLICATION
TIER
130
DATABASE
TIER
140
CLIENT
(E.G., BROWSER)
110
160
APPLICATION
SERVER
120
170
DATABASE SERVER
150

FIGURE 1

Figure 2


200
CRYPTOGRAPHIC DEVICE 201
206
205
SECURE KEY GENERATOR 202
207
208
TRANSMITTER RECEIVER 209
INSECURE CHANNEL 210
204
KEY SOURCE 203
TRANSMITTER RECEIVER 211
215
CRYPTOGRAPHIC DEVICE 216
221
220
SECURE KEY GENERATOR 217
223
222
219
KEY SOURCE 218

Attorney Docket No. 5036.P005

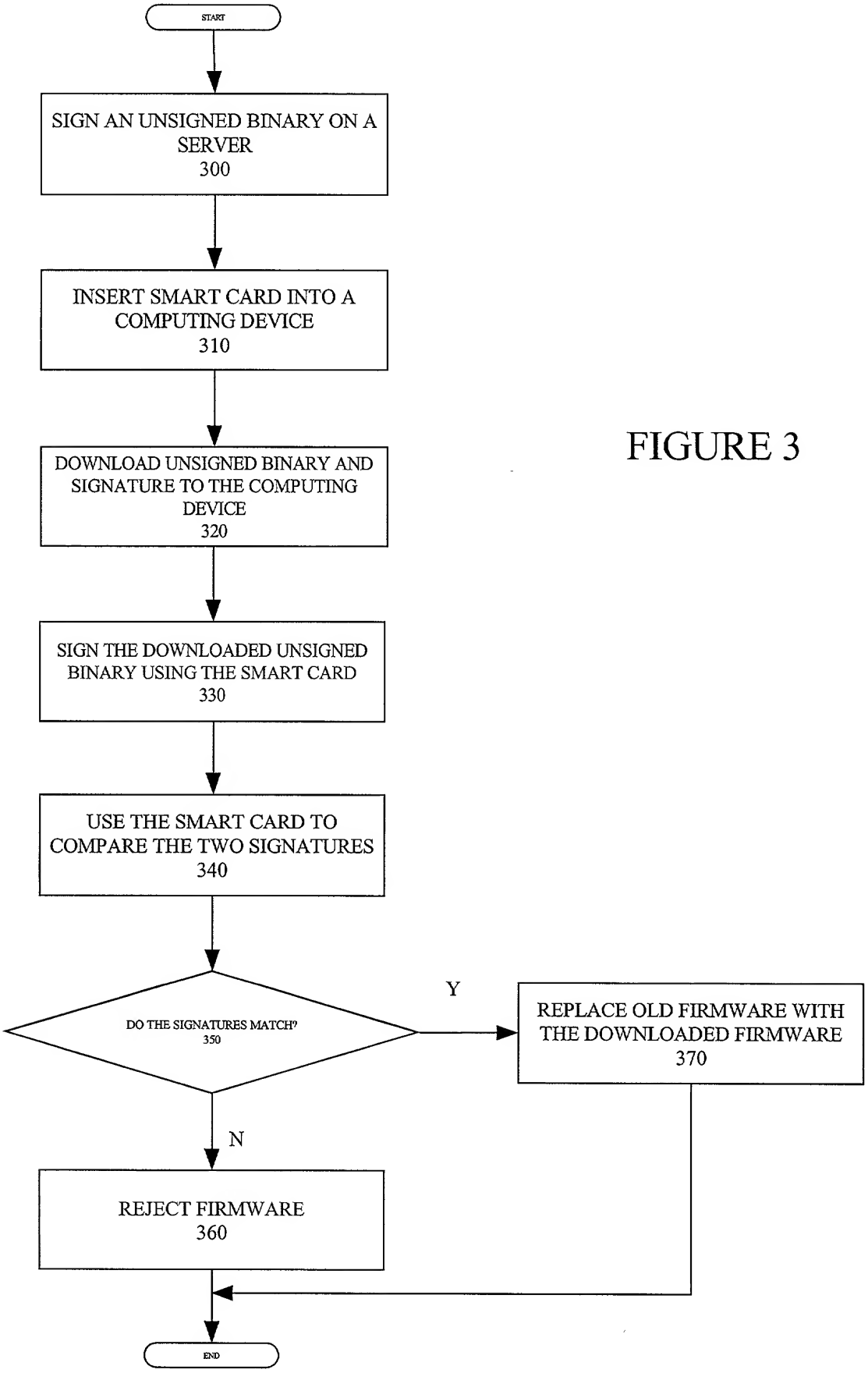


FIGURE 3

Post-Grant Publication

FIGURE 4

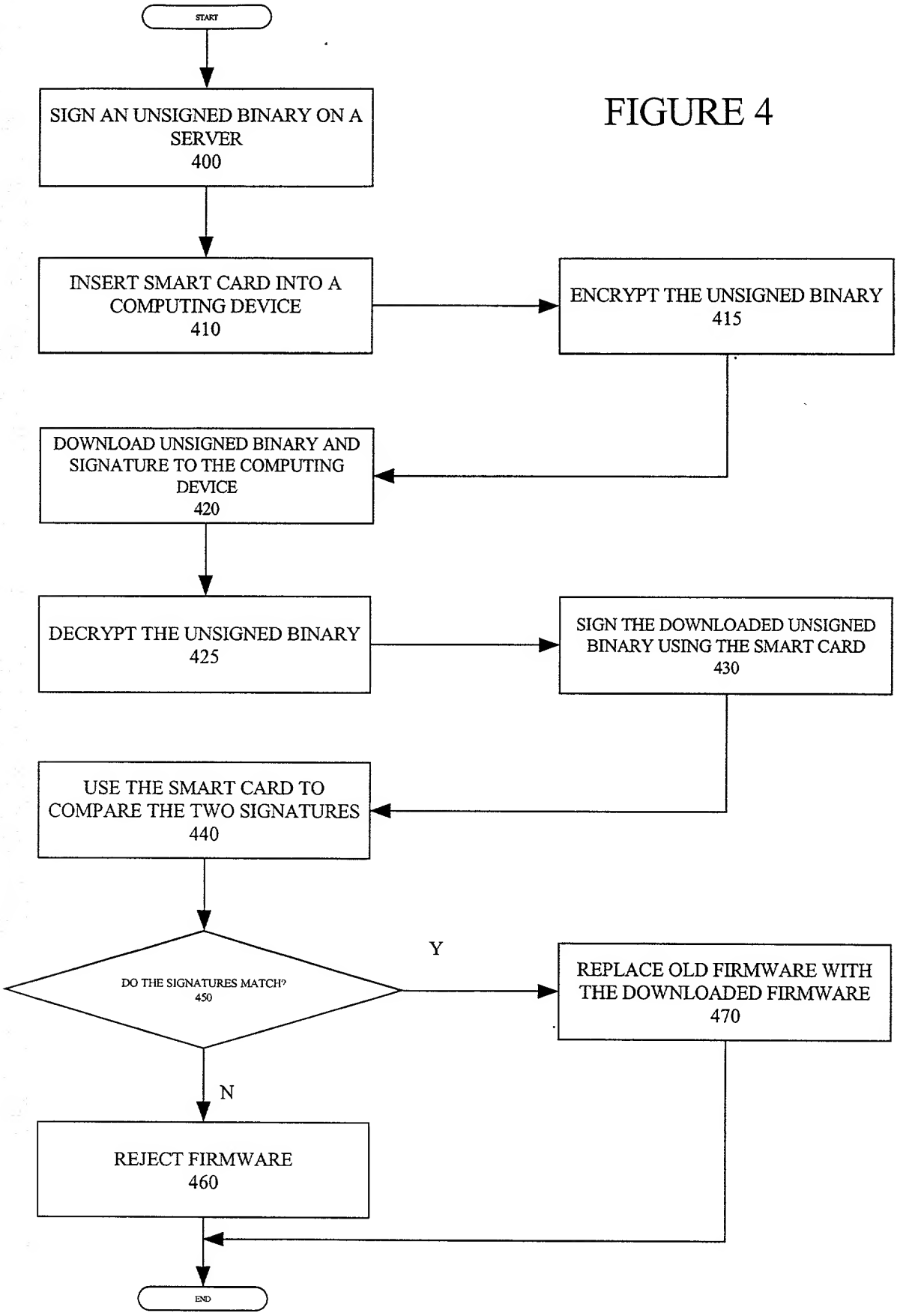


FIGURE 5

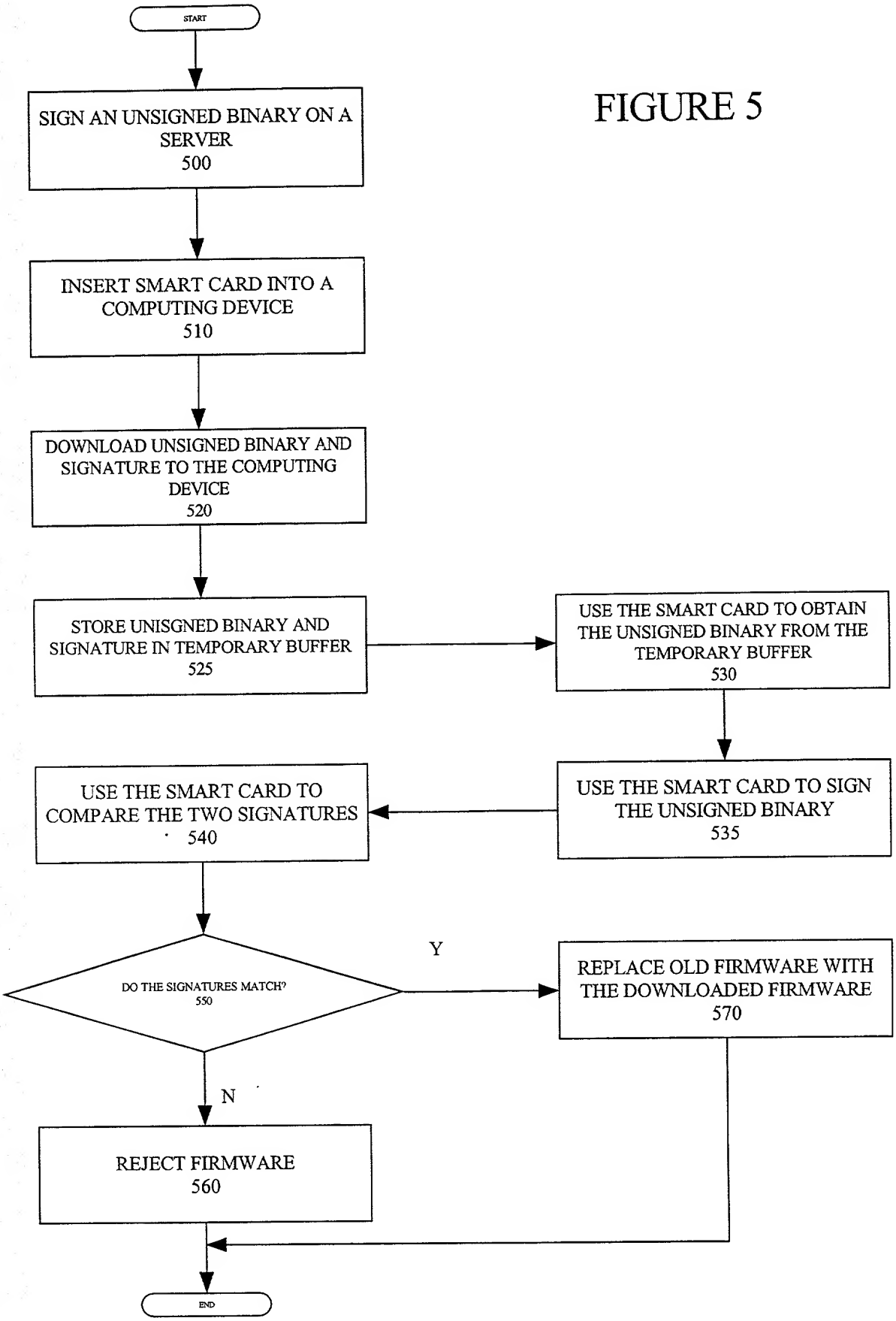
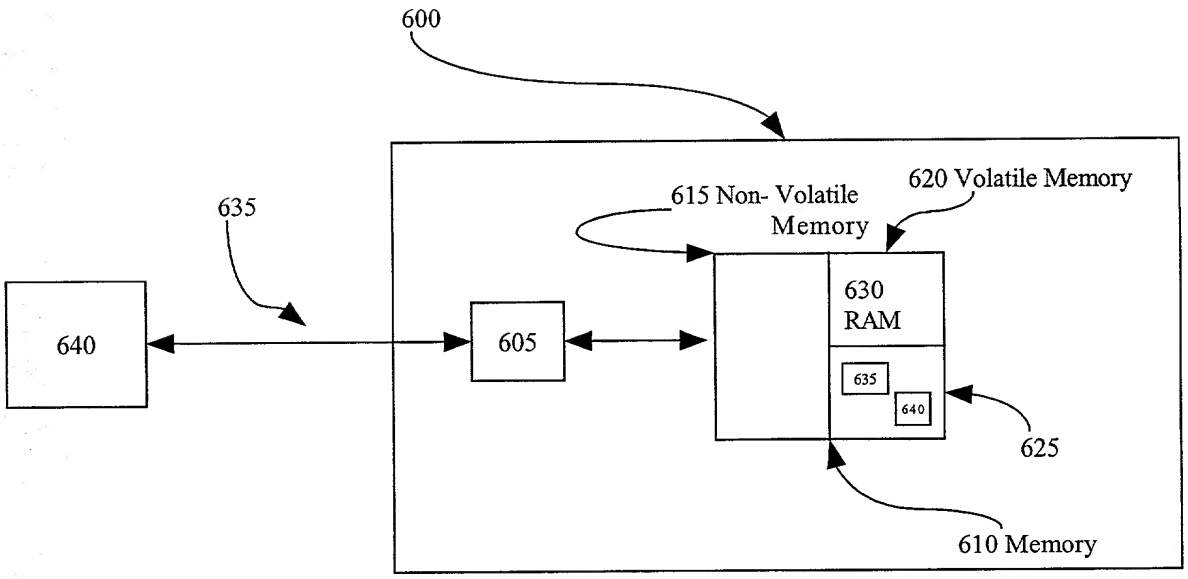

START
SIGN AN UNSIGNED BINARY ON A SERVER
500
INSERT SMART CARD INTO A COMPUTING DEVICE
510
DOWNLOAD UNSIGNED BINARY AND SIGNATURE TO THE COMPUTING DEVICE
520
STORE UNISGNED BINARY AND SIGNATURE IN TEMPORARY BUFFER
525
USE THE SMART CARD TO OBTAIN THE UNSIGNED BINARY FROM THE TEMPORARY BUFFER
530
USE THE SMART CARD TO SIGN THE UNSIGNED BINARY
535
USE THE SMART CARD TO COMPARE THE TWO SIGNATURES
540
DO THE SIGNATURES MATCH?
550
Y
REPLACE OLD FIRMWARE WITH THE DOWNLOADED FIRMWARE
570
N
REJECT FIRMWARE
560
END

FIGURE 6


600
635
615 Non- Volatile Memory
620 Volatile Memory
640
605
630 RAM
635
640
625
610 Memory

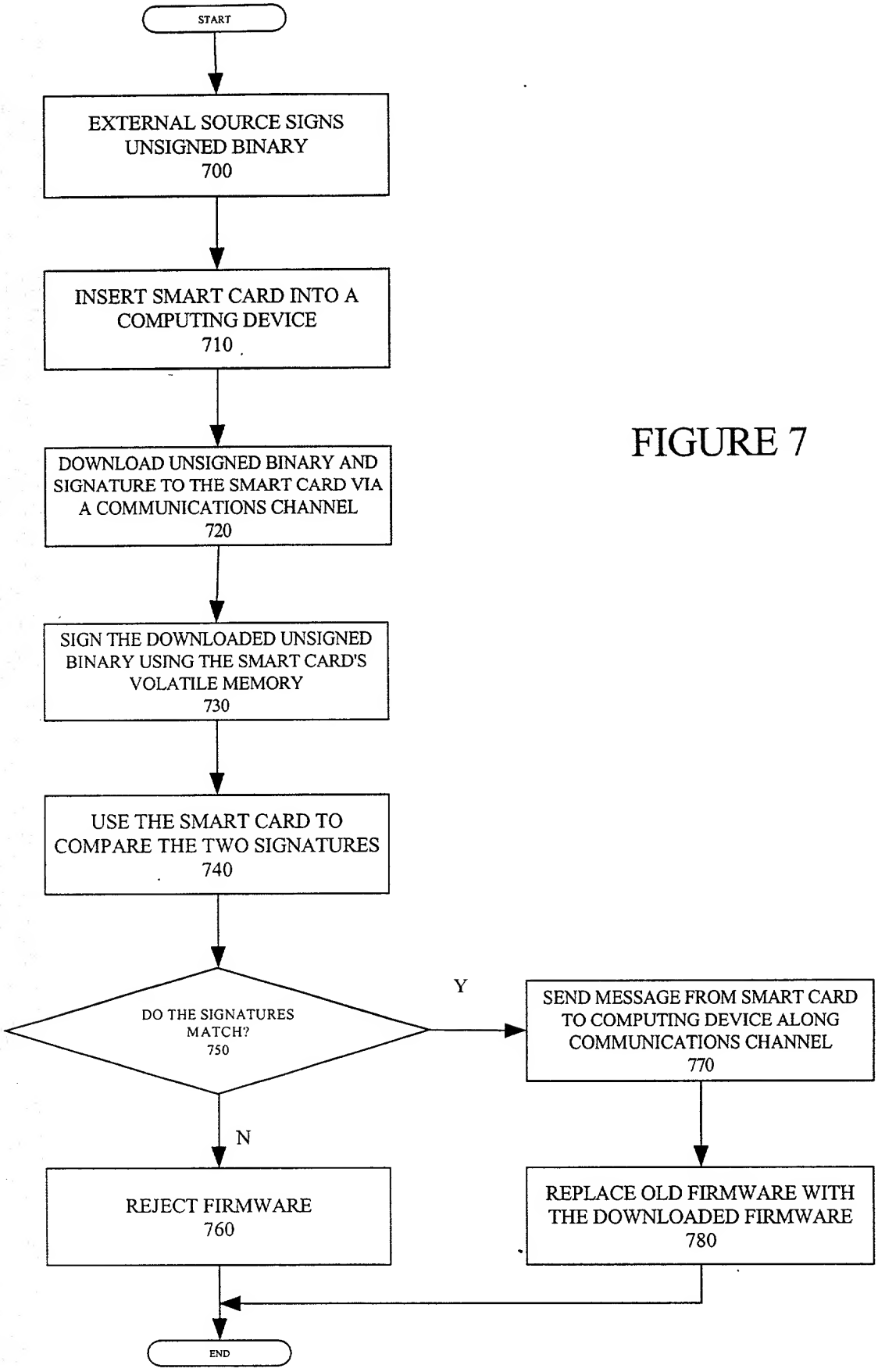

START
EXTERNAL SOURCE SIGNS UNSIGNED BINARY 700
INSERT SMART CARD INTO A COMPUTING DEVICE 710
DOWNLOAD UNSIGNED BINARY AND SIGNATURE TO THE SMART CARD VIA A COMMUNICATIONS CHANNEL 720
SIGN THE DOWNLOADED UNSIGNED BINARY USING THE SMART CARD'S VOLATILE MEMORY 730
USE THE SMART CARD TO COMPARE THE TWO SIGNATURES 740
DO THE SIGNATURES MATCH? 750
Y
N
SEND MESSAGE FROM SMART CARD TO COMPUTING DEVICE ALONG COMMUNICATIONS CHANNEL 770
REPLACE OLD FIRMWARE WITH THE DOWNLOADED FIRMWARE 780
REJECT FIRMWARE 760
END

FIGURE 7

PCT/GB2005/004005

Figure 8

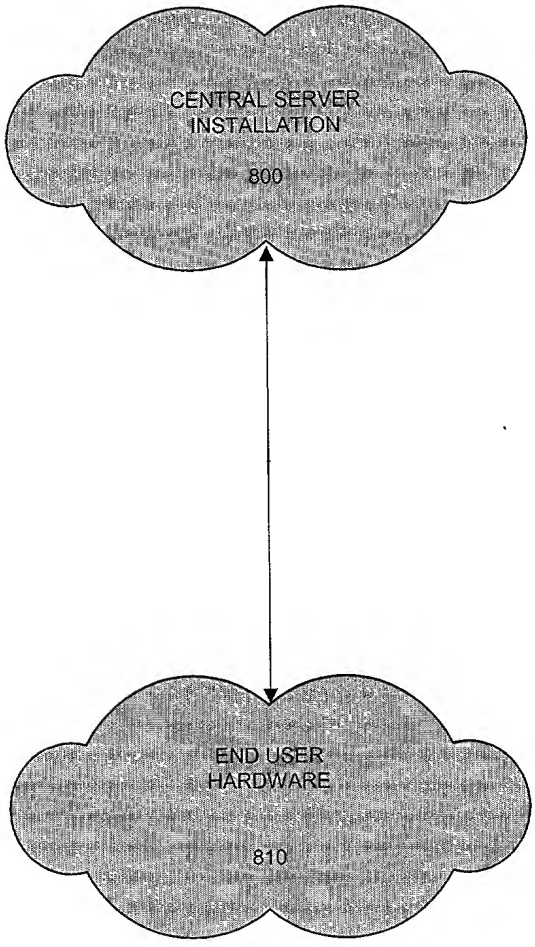


Figure 9

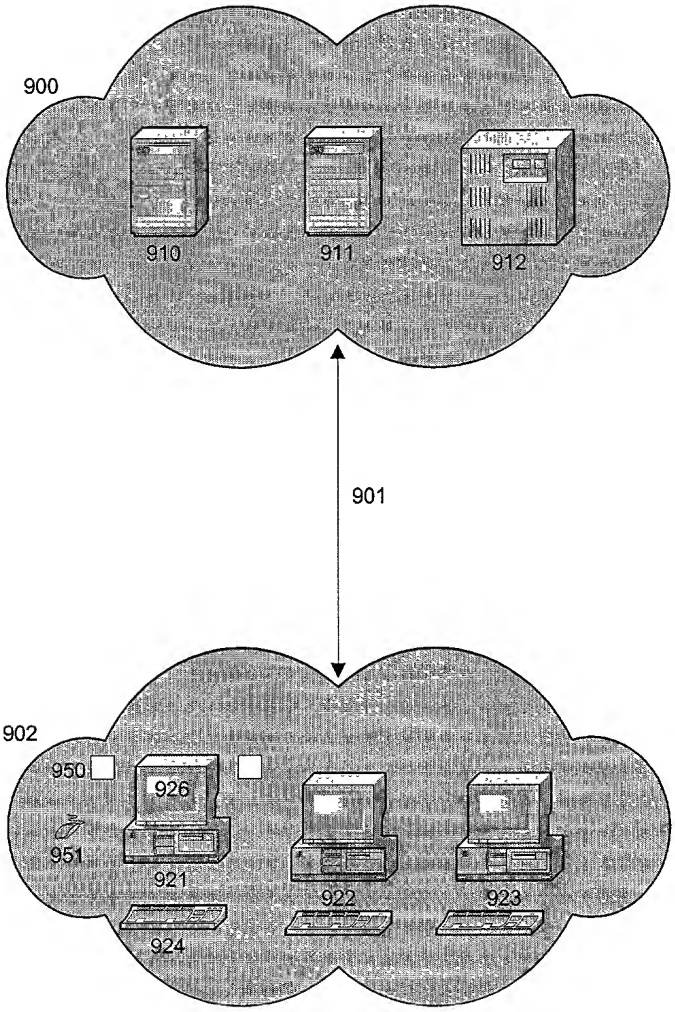


Figure 10:
HID

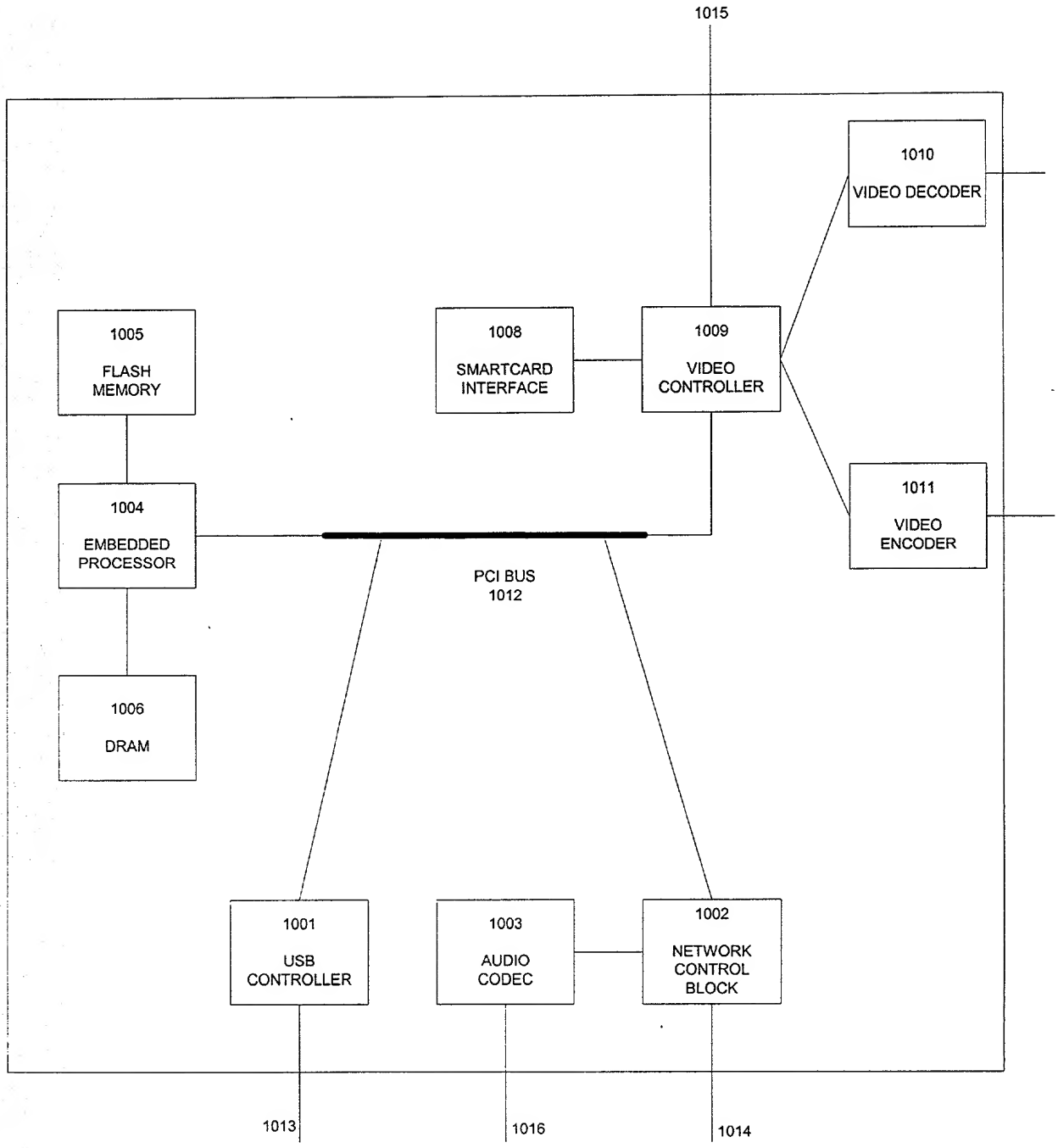
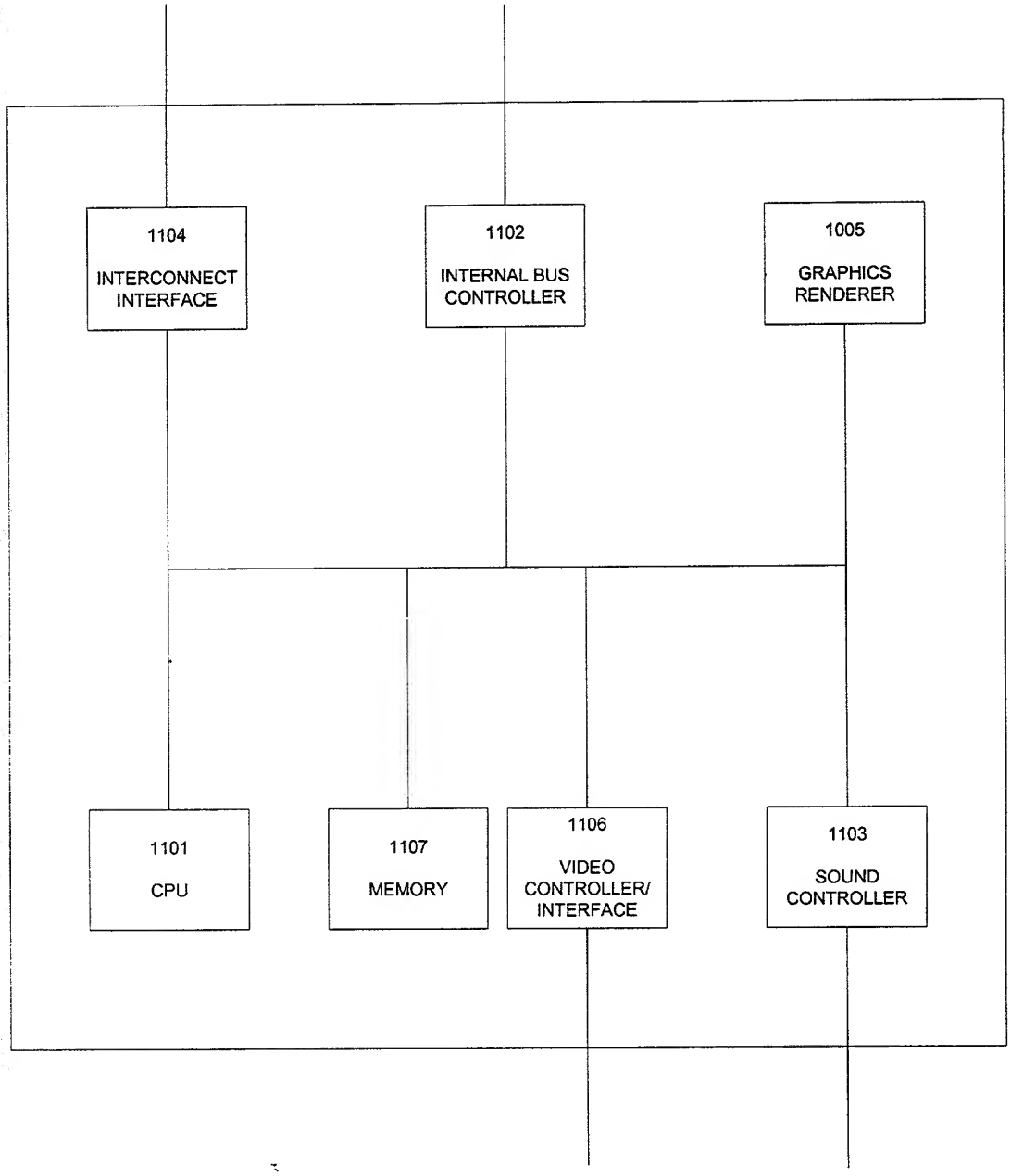


Figure 11:
HID SINGLE CHIP IMPLEMENTATION



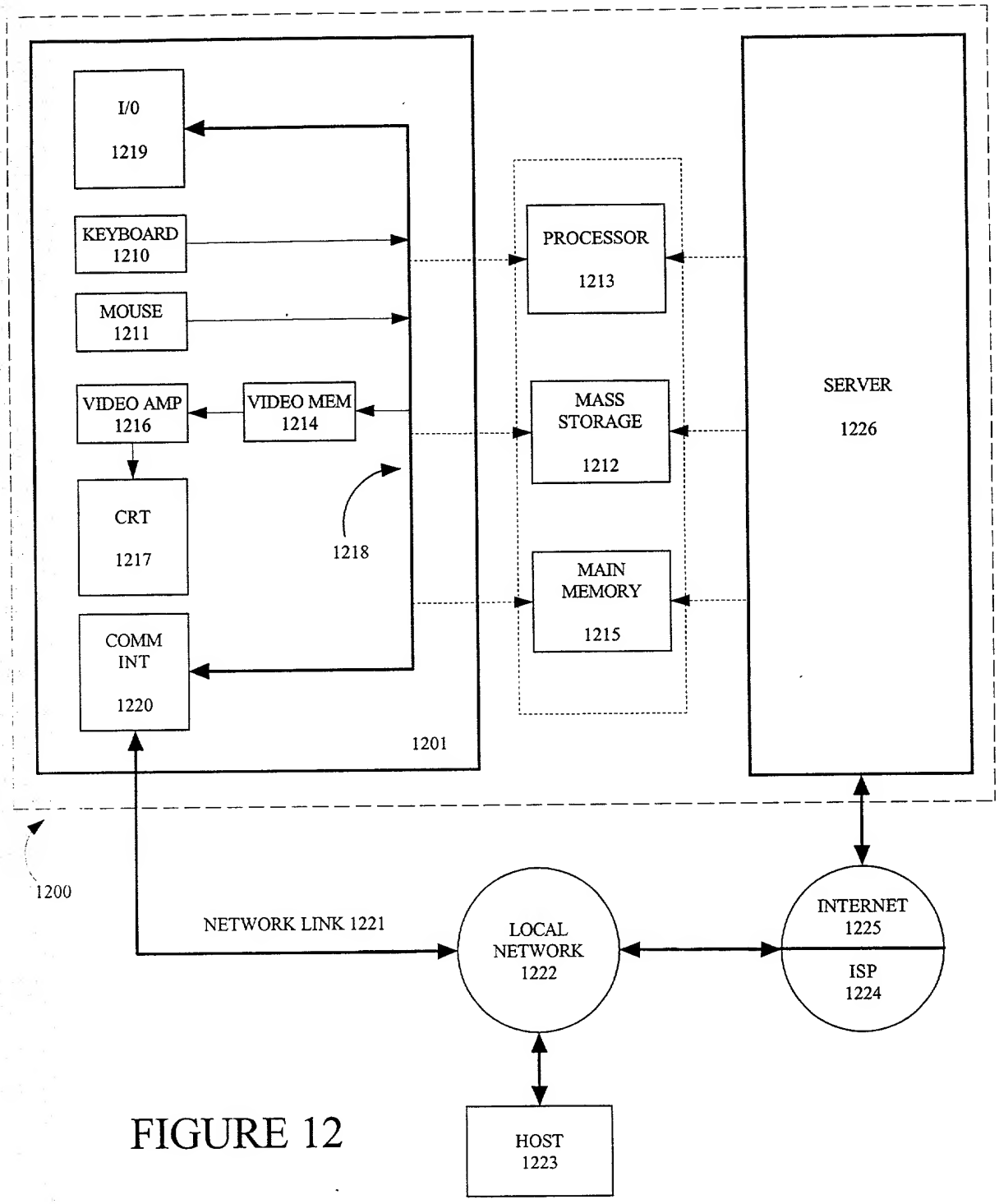

I/O
1219
KEYBOARD
1210
MOUSE
1211
VIDEO AMP
1216
VIDEO MEM
1214
CRT
1217
COMM
INT
1220
1218
1201
PROCESSOR
1213
MASS
STORAGE
1212
MAIN
MEMORY
1215
SERVER
1226
1200
NETWORK LINK 1221
LOCAL
NETWORK
1222
INTERNET
1225
ISP
1224
HOST
1223

FIGURE 12